Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of Release of Customer Information During 9-1-1 Emergencies	RM – 10715

COMMENTS OF THE CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION

Michael F. Altschul
Senior Vice President, General Counsel

CELLULAR TELECOMMUNICATIONS
& INTERNET ASSOCIATION
1250 Connecticut Ave., NW Suite 800
Washington, DC 20036
(202) 785-0081

Dated: August 15, 2003

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of Release of Customer Information During 9-1-1 Emergencies	RM – 10715

COMMENTS OF THE CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION

The Cellular Telecommunications & Internet Association ("CTIA")[1] hereby submits its comments in response to the Commission's Public Notice[2] regarding the petition for rulemaking recently filed by the National Emergency Number Association, the Association of Public-Safety Communications Officials International, Inc., and the National Association of State Nine One One Administrators (collectively "Petitioners") in the above-captioned proceeding.[3] Petitioners urge the Commission to clarify "the legal preconditions to release of customer-specific information to Public Safety Answering Points ("PSAPs") in the course of

---

[1] CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers all Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, broadband PCS, ESMR, as well as providers and manufacturers of wireless data services and products.

[2] *Comment Sought on Petition for Rulemaking on Compliance by Carriers with Relevant Statutory Provisions on Disclosure of Customer Information in 911 Emergencies*, Public Notice, RM-10715, DA 03-1952 (rel. June 16, 2003).

[3] *Release of Customer Information During 9-1-1 Emergencies*, Petition for Rulemaking, RM-10715 (filed May 2, 2003) ("*Petition*").

response to 9-1-1 emergency calls."[4] Petitioners also seek to broaden the consent exception to permit disclosure of the customer information of subscribers *other* than the 911 caller.[5] And Petitioners argue for expansion of ECPA to include emergencies relating to destruction of property.[6]

CTIA agrees with Petitioners that "seconds matter" and is proud that wireless carriers have demonstrated their commitment to cooperating with public safety entities in emergency situations. CTIA shares the concerns of Petitioners as CTIA's members are often caught in the middle between a PSAP's demand for more information and a carrier's obligation to protect customer privacy. As described below, the statutory provisions governing the disclosure of customer specific information are set forth both in Section 222 of the Communications Act of 1934, as amended, ("Communications Act") and in the Electronic Communications Privacy Act ("ECPA").[7] While the Commission may interpret carriers' obligations under the relevant provisions of the Communications Act, it has no authority to alter Congress's framework for protecting customer information from disclosure.

---

[4] *Id.* at 1.

[5] *See id.* at 5-6.

[6] *See id*. at 5 ("It makes little sense to differentiate the disclosure of customer information based on whether property or lives may be at risk.").

[7] Where the statutory framework permits, such disclosures may also be governed by a carrier's privacy policy published in accordance with the principles established by the Federal Trade Commission. The FTC deems publication of these policies to create a legally enforceable obligation.

I. INTRODUCTION

In the post-September 11th world, we are all aware of the challenges faced by providers of emergency services, and wireless carriers have demonstrated their willingness to assist these "first responders" where such assistance is not otherwise precluded by a carrier's obligation to protect customers' information from disclosure. A carrier's ability to respond to PSAP requests for customer specific information is limited, however, by a careful framework established by Congress that limits governmental access to certain customer information and authorizes service providers *only in certain specified emergency cases* to disclose customer information without the legal process government agencies otherwise would be required to obtain. This statutory framework grants service providers a significant amount of discretion in guarding against the unauthorized disclosure of certain customer information and, most importantly, protects these providers from liability for such disclosures when the provider meets the requirements of the law. This framework was reviewed and amended after September 11th and reflects the judgment of Congress on the appropriate balance between disclosure of private customer information and emergency needs. Accordingly, Petitioners concerns ultimately should be raised with Congress, not the Commission.

II. THE LEGAL FRAMEWORK

The CPNI provisions of the Communications Act, 47 U.S.C. § 222, and the ECPA, 18 U.S.C. § 2701 *et seq.,* as well as the Commission's own rules, regulate the disclosure of customer information. There are four relevant bases for disclosure of customer information: (1) **mandatory** disclosure of certain limited information to emergency service providers; (2) **compelled** disclosure by legal process to law enforcement agencies; (3) **consensual** disclosure when the customer requests it; and (4) **voluntary** service provider disclosure when authorized by law.

A. Mandatory Disclosure

Mandatory disclosure of customer information to emergency service providers is governed by the Wireless Communications and Public Safety Act of 1999 ("WCPSA"),[8] which amended Section 222 of the Communications Act. While these amendments to the Communications Act addressed important needs of the emergency services community, the scope of what this legislation actually requires service providers to disclose is quite limited.

Section 222 of the Communications Act sets forth protections for customer proprietary network information ("CPNI"), which includes the quantity, duration, and location of a customer's telecommunications use, but not basic subscriber information. Generally, a carrier may not release CPNI without the customer's authorization or legal process, but the WCPSA added new section 222(g) to mandate certain disclosures as follows:

> **(g) Subscriber listed and unlisted information for emergency services.** Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i)(3)(A) [(h)(3)(A)] (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

Thus, telecommunications carriers that provide telephone exchange service or comparable service[9] must provide "subscriber listed and unlisted information"[10] (*i.e.,*

---

[8] Wireless Communications and Public Safety Act of 1999, P.L. 106-81, 1999 U.S.C.C.A.N. (113 Stat.) 1286.

[9] The Commission has interpreted this language to include cellular, broadband PCS and covered SMR service providers because they "provide local, two-way switched voice service as a principal part of their business." *See In the Matter of Implementation of the Telecommunications Act of 1996, Interconnection between Local Exchange Carriers and Commercial Mobile Radio Service*

subscriber names, telephone numbers, and addresses) to emergency service providers upon request.[11]

The Commission's E911 rules also explicitly require wireless carriers to transmit every 911 call to a PSAP and provide appropriately equipped PSAPs with a caller's telephone number and location.[12] Wireless carriers have expended significant resources complying with this mandate and are deploying (or have deployed) technology to route 911 calls and the required location information to the appropriate PSAP. Thus, while a wireless carrier *must* automatically transmit location information to a PSAP that is capable of receiving it as part of the 911 call, there is no Commission *requirement* to disclose this location information such as in response to a telephonic request from an agency or family member who asserts an emergency.[13]

Providers, First Report and Order, CC Docket Nos. 95-185 & 96-98, 11 FCC Rcd 15499, 15999 at ¶ 1013 (1996).

[10] "Subscriber list information" is expressly excluded from the definition of "customer proprietary network information." 47 U.S.C. §§ 222(h)(1), (3). Transmission of a subscriber's name and number is consistent with the Commission's view that this information does not implicate the same privacy concerns related to CPNI. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order, 13 FCC Rcd 12390, 12395 (1998) (clarifying that a "customer's name, address, and telephone number do not fall within the definition of CPNI"). The Commission has found that transmission of information about a caller's name and telephone number is "far less sensitive than the disclosure of CPNI." *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8136 (1998).

[11] Carriers typically comply with this requirement by providing a database to PSAPs rather than requiring the emergency service providers to obtain this information on a per dip, per call basis.

[12] 47 C.F.R. § 20.18.

[13] While CTIA does not challenge the lawful basis for the Commission's automatic location information ("ALI") requirement, it is worth noting that the WCPSA, enacted in 1999, does not *require* but merely *permits* wireless carriers to provide such information to PSAPs and others.

It is important to note from a privacy perspective that mandatory disclosures occur without the prior notice or consent of the customer. The law simply mandates the disclosure.[14]

B. Compelled Disclosure

ECPA generally prohibits service providers from releasing subscriber records or other information to any governmental entity without lawful process.[15] If the government wants customer records that include name, address, phone number, call records, length and type of service, and means and source of payment, ECPA requires that the government serve the service provider with, at minimum, a subpoena.[16] Disclosure of other information, such as location information from a wireless communications provider, requires the government to obtain a court order for disclosure based on specific and articulable facts that the information is relevant and material to an ongoing criminal investigation.[17]

ECPA does not distinguish PSAPs or other government emergency response personnel from other law enforcement entities. All governmental agencies are restricted in their access to customer information by ECPA and service providers that fail to observe ECPA's strictures may be subject to both civil and criminal penalties.[18] Conversely, service

---

[14] Mandatory disclosure without prior notice or consent places control of the personal information beyond the customer. For that reason alone, the Commission should ensure that the mandatory disclosure law is construed narrowly not to mention the fact that disclosure is a limited exception to the general prohibition on disclosure, which, as a matter of statutory construction, must be viewed narrowly. *See, e.g., Communications Assistance for Law Enforcement Act*, Second Order on Reconsideration, CC Docket No. 97-213, 16 FCC Rcd 8959, at ¶ 17 (2001) (construing CALEA narrowly and denying FBI's request that FCC require carriers to safeguard security and intercept activities in a specific manner because the statutory scheme left how this may be done to the carrier's discretion).

[15] *See* 18 U.S.C. § 2702(a)(1); 18 U.S.C. § 2702(a)(3).

[16] 18 U.S.C. § 2703(c).

[17] 18 U.S.C. § 2703(d).

[18] 18 U.S.C. § 2707.

providers that rely on, and act in accordance with, legal process are immunized from suit.[19] Thus, service providers have a strong incentive to protect against unlawful disclosure of customer records and to rely on legal process in responding to any governmental request for such information.

Section 222 of the Communications Act is perfectly congruent with ECPA on this score. Minus limited exceptions, it permits disclosure of CPNI only "except as required by law or with the approval of the customer."[20]

C. Customer Consent

Both ECPA and Section 222 of the Communications Act permit disclosure of customer information with the customer's consent.[21] In regard to disclosure of emergency location information, the Department of Justice ("DoJ") has opined that a 911 caller *impliedly* consents to disclosure of a caller's physical location at the time of a 911 call under Section 2703(c) of ECPA.[22]

---

[19] 18 U.S.C. § 2703(e).

[20] 47 U.S.C. § 222(c)(1).

[21] 18 U.S.C. § 2703(c)(1)(C); 47 U.S.C. § 222(c)(1).

[22] *Memorandum Opinion to Criminal Division from Office of Legal Counsel*, Department of Justice (Sept. 10, 1996) at 5-6 ("*DoJ Opinion*"). In light of the Commission's subsequent analysis of the form of approval required from the customer to disclose CPNI; *see Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Clarification Order and Second Further Notice of Proposed Rulemaking, 16 FCC Rcd 16506, at ¶¶ 7-11 (2001), or to receive marketing communications under Section 227 of the Act, the DOJ Opinion must be read narrowly as applying solely to disclosure of a caller's physical location under Section 2703(c) of ECPA. *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, FCC 3-153, at ¶¶ 100-107 (rel. July 3, 2003).

Petitioners seek to broaden the consent exception to permit disclosure of the customer information of subscribers *other* than the 911 caller.[23] The Petition includes what Petitioners contend is a typical scenario where a worried friend or relative calls 911.[24] The attorney for the carrier responded correctly to the scenario by noting that WCPSA *only* permits disclosure of location information of a *user's* call for emergency purposes.[25] Only a subscriber to a service can consent to the disclosure of his or her records and the DoJ Opinion says no more than that.

Under ECPA, consent is a narrow exception to the general prohibition on disclosure of customer information.[26] The Commission's own rulemaking on CPNI under Section 222 follows the same approach.[27] There is no need to expand the consent exception to accomplish Petitioner's goals – in those cases where a third party calls an emergency service provider to report a suspected emergency, that agency can obtain a subpoena to compel disclosure of the information if it meets the statutory standard. If it does not meet the standard, an *ipse dixit* declaration of an "emergency" to facilitate the investigation should not be used as a substitute. Any other result runs counter to the Commission's efforts to safeguard customers' CPNI and needlessly places carriers at risk of violating their subscribers' privacy rights.

---

[23] *See Petition* at 5-6.

[24] Concerned third parties will also contact wireless carriers directly to seek this type of subscriber information.

[25] *See Petition* at 5-6.

[26] *See Blumofe v. Pharmatrak Inc.,* 329 F.3d 9, 20 (1st Cir. May 9, 2003) (finding users of websites bringing ECPA action did not consent to collection of their personal information because websites gave no indication that use meant consent).

[27] *See supra* note 22.

D. Voluntary Disclosures

In the wake of September 11th, Congress amended ECPA twice to provide exceptions to the general prohibition on disclosure of customer records. The USA Patriot Act of 2001 ("USPA")[28] and Homeland Security Act of 2002 ("HSA")[29] both carve out exceptions to the general prohibition and permit service providers to disclose subscriber information to emergency personnel in limited emergencies involving imminent bodily harm or death. Accordingly, ECPA now *permits,* but does not compel, a service provider to disclose a "record or other information pertaining to a subscriber to or customer" to a governmental entity, if the "provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[30]

Prior to September 11th, with the enactment of WCPSA, telecommunications carriers also were permitted, but not required, to disclose "call location information concerning the user of a commercial mobile service" to: a PSAP or other specified emergency personnel; the user's family in an emergency situation that involves the risk of death or serious physical harm; or to providers of information or database management services solely for purposes of assisting in the delivery of emergency services.[31] Prior to WCPSA, there was no legal authority to disclose *any* customer information to a PSAP in an emergency situation without customer consent or legal process. Carriers often relied on tariffs, implied consent, permission in terms and conditions for service, or the good graces of the customer not to complain when disclosing such information.

---

[28] Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, P.L. 107-56, 2001 U.S.C.C.A.N. (115 Stat.) 272.

[29] Homeland Security Act of 2002, P.L. 107-296, 2002 U.S.C.C.A.N. (116 Stat.) 2135.

[30] 18 U.S.C. § 2702(c)(4).

[31] 47 U.S.C. §§ 222(d)(4)(A)-(C).

With the passage of the USPA and the HSA, service providers now have immunity from suit when "providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under [ECPA]."[32] Thus, as noted above, a service provider that "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information" has protection under ECPA.[33]

Petitioners argue for expansion of ECPA to include emergencies relating to destruction of property because, as Petitioners assert, differentiating between emergencies involving life versus property "makes little sense."[34] Maybe so. But it is hard to argue that Congress was unaware of the great property destruction caused by the September 11th attacks. That Congress nonetheless kept the exception for emergency disclosure narrow speaks volumes about Congressional intent even if the words "death or serious physical injury" somehow could be read to be ambiguous. Unfortunately, as noted above, the Commission lacks authority to modify ECPA in this regard. Here again, Petitioners complaint is better addressed to Congress.

Finally, CTIA agrees with Petitioners that emergency calls are often highly pressurized situations; where seconds do indeed count. As such, carriers cannot be expected to have their employees make discrete, spot assessments regarding whether a caller purporting to be a PSAP or family member is genuinely responding to an emergency, and

---

[32] 18 U.S.C. § 2703(e).

[33] 18 U.S.C. § 2707(e)(1). While a service provider might have an affirmative defense in a civil action based on its good faith reliance on Section 222(g), which could be viewed as conflicting with ECPA's Section 2703, Congress has not provided the Commission authority to immunize carriers from liability or otherwise protect carriers that followed a disclosure rule that is in conflict with ECPA's general prohibition on records disclosure.

[34] *Petition* at 5.

leave to chance or future litigation whether the carrier's reliance on this assessment in disclosing was "reasonable."

III. CONCLUSION

For the reasons discussed herein, the Commission lacks jurisdiction to alter the scope of a wireless carrier's obligation to provide customer information to emergency service providers. Therefore, the Commission should deny the Petitioners request for rulemaking or declaratory order.

Respectfully submitted,

/s/ Michael F. Altschul
Michael F. Altschul
Senior Vice President, General Counsel

CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION
1250 Connecticut Ave., NW
Suite 800
Washington, DC 20036
(202) 785-0081

Date: August 15, 2003